

Audit Report



TRACKING SECURITY CLEARANCE REQUESTS

Report No. D-2000-134

May 30, 2000

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CCMS	Case Control Management System
DSS	Defense Security Service
ESP	Extranet for Security Professionals



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2885

May 30, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Audit Report on Tracking Security Clearance Requests
(Report No. D-2000-134)

We are providing this report for review and comment. This report is the third in a series of audit reports addressing security clearance and access issues. We considered management comments on a draft of this report when preparing the final report.

Management comments were sufficiently responsive and no further comments on the final report are required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (rwest@dodig.osd.mil) or Ms. Lois A. Therrien at (703) 602-1577 (DSN 332-1577) (ltherrien@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the printed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2000-134
(Project No. 9AD-0046.04)

May 30, 2000

Tracking Security Clearance Requests

Executive Summary

Introduction. This report is the third in a series of audit reports addressing security clearance and access issues.

Objectives. During our audit to determine the status of actions taken within DoD relating to access reciprocity between special access programs, we identified problems with obtaining security clearances that affected individuals' access to special access programs and other DoD operations. As a result, this report addresses the effectiveness of the Defense Security Service process for tracking security clearance requests. We also reviewed the adequacy of the management control program as it applied to the specific audit objective. We addressed the impact of obtaining background investigations for security clearances on three special access programs in Inspector General, DoD, Report No. D-2000-072, "Expediting Security Clearance Background Investigations for Three Special Access Programs" (U), January 31, 2000 (SECRET), and whether security clearances were being obtained and updated for personnel in the most critical and high-risk positions in the draft report for Inspector General, DoD, Project No. 9AD-0046.03, "Security Clearance Investigative Priorities," January 31, 2000. Future audit reports will cover the adjudication process, the impact of security clearances on all special access programs and access reciprocity, and the acquisition of the Case Control Management System.

Results. The Defense Security Service lacks an effective process for tracking security clearance requests. Between July and December 1999, the Defense Security Service could not identify, on a case-by-case basis, why 12,354 of 302,352 electronic requests received did not result in investigative cases. The Defense Security Service provided possible reasons such as changes in type of investigation, duplicate submissions, conversions and reinstatements of prior clearances, and rejections. Also, the Defense Security Service could not specifically identify why 51,788 of 261,361 investigative cases were opened during that period without electronic requests. The Defense Security Service attributed these cases to changes in type of investigation, requests received in paper rather than electronically, and cases being reopened because of additional information requested by the adjudicative facility. Other confusing factors included case analysts manually entering paper requests submitted into the Case Control Management System; requesting agencies submitting duplicate requests that case analysts had to manually annotate as deleted; and the lack of active acknowledgement of request receipts, which created the appearance that requests were being lost. The Defense Security Service acknowledged that its case analysts spent an excessive amount of their time researching the status of requests. For details of the audit results, see the Finding section of this report. See Appendix A for details of the review of the management control program.

Summary of Recommendations. We recommend that the Director, Defense Security Service, track all security clearance requests from the time they are received until the investigative cases are opened and post all cases in process on the Extranet for Security Professionals.

Management Comments. The Defense Security Service and the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with the recommendation to track all security clearance requests from the time they are received until the investigative cases are opened. The Defense Security Service concurred with the recommendation to post the names and social security numbers of all cases in process, but stated that the dates an investigation is opened and closed are posted in the Defense Clearance and Investigations Index database, which is available to authorized users. In addition, the Defense Security Service has established a site on its web site, which posts daily and maintains for 120 days an index of all electronic requests received. The Defense Security Service will evaluate the feasibility of modifying the Case Control Management System to address this problem.

The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) partially concurred with the recommendation to post the names and social security numbers of all cases in process, stating it agrees there should be a mechanism to monitor the status of investigations; however, the Joint Personnel Adjudication System, due to be implemented in the near future, would provide the capability to monitor requested investigations and meet the intent of the recommendations. A discussion of the management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Audit Response. Management comments were generally responsive. DoD contractors do not have access to the Defense Clearance and Investigations Index and the Defense Security Service web site does not contain information on the status of cases or the manually entered paper requests. Therefore, an inordinate amount of time would continue to be spent by Defense Security Service personnel investigating the status of requests. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) recommended using the Joint Personnel Adjudication System, which we agree ought to be the long-term solution. Because the Joint Personnel Adjudication System is not scheduled to be fully operational until FY 2002, however, it would be advisable to move ahead with interim corrective action. We will follow up on this point in our ongoing audit of the Case Control Management System.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objectives	2
Finding	
Tracking Security Clearance Requests	4
Appendixes	
A. Audit Process	
Scope	13
Methodology	13
Management Control Program	14
B. Prior Coverage	15
C. Auditor Calculations of Pending Cases	16
D. Report Distribution	22
Management Comments	
Defense Security Service	25
Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	27

Background

This report is the third in a series and discusses security clearance requests. The first report discussed the effects of security clearances on three special access programs. The second report discussed security clearances for personnel in mission-critical and high-risk positions. Subsequent reports will discuss the adjudication process, the effects of security clearances on all special access programs and the status of access reciprocity, and the acquisition of the Case Control Management System.

Security Clearances. Personnel security clearance investigations are intended to establish and maintain a reasonable threshold for trustworthiness through investigation and adjudication before granting and maintaining access to classified information. The initial investigation provides assurance that a person has not demonstrated behavior that could be a security concern. Reinvestigation is an important, formal check to help uncover changes in behavior that occurred after the initial clearance was granted. The standard for reinvestigation is 5 years for Top Secret, 10 years for Secret, and 15 years for Confidential clearances. Reinvestigations are more important than the initial clearance investigation, because people who have held clearances longer are more likely to be working with more critical information and systems.

Clearance Requirements. On March 24, 1997, the President approved the uniform Adjudicative Guidelines and Temporary Eligibility Standards and Investigative Standards, as required by Executive Order 12968, "Access to Classified Information." The investigative standards dictate that the initial investigation and reinvestigation for access to Top Secret and Sensitive Compartmented Information are the single-scope background investigation and the single-scope background investigation periodic reinvestigation, respectively. The investigation and reinvestigation for access to Secret and Confidential information consists of a national agency check, with local agency checks, and a credit check.

DoD Security Clearances. The process of obtaining a security clearance begins with a request from a military commander, contractor, or other DoD official for a security clearance for an individual because of the sensitive nature of his or her duties. The individual then completes a security questionnaire that is forwarded to the DSS Personnel Investigations Center, in Linthicum, Maryland. The Center's case analysts review clearance requests to determine whether all necessary forms are complete, develop a scope for the investigation, and assign the required work to the 12 DSS operating locations throughout the United States. An investigation may be sent to one or more operating locations depending on where the individual seeking the clearance lived, worked, or attended school. Once received in the field, an investigation is assigned to an investigator who seeks information in that geographic location about the subject's loyalty, character, reliability, trustworthiness, honesty, and financial responsibility. The investigation must be expanded to clarify and resolve any information that raises questions about the subject's suitability to hold a position of trust. As investigative elements are completed, the field sends reports to the DSS Personnel Investigations Center, in Linthicum, Maryland, where case

analysts determine whether all investigative criteria have been met and whether all relevant issues have been resolved. The case analysts also request information from other Federal agencies, such as the Office of Personnel Management, the Federal Bureau of Investigation, the Central Intelligence Agency, and the Immigration and Naturalization Service. DSS sends the completed investigation to the appropriate adjudication facility, which decides whether to grant a clearance.

Defense Security Service. DSS has three missions: personnel security investigations; industrial security; and security education, training, and awareness. The mission of personnel security investigations is to conduct background investigations on individuals assigned to or affiliated with DoD. Military and civilian personnel security investigations are processed at the DSS Personnel Investigations Center. Industrial or contractor security clearances are processed at the Defense Industrial Security Clearance Office.

Case Control Management System. The Case Control Management System (CCMS) was set up to expedite case processing at DSS by linking all relevant information that is critical to a background investigation through a series of subsystems. These subsystems include:

- the Electronic Personnel Security Questionnaire, which electronically collects the personnel security data to initiate and conduct an investigation;
- the Field Information Management System, which generates field investigative reports that are then fed into the system;
- the Files Automation Scanning System, which converts paper personnel security questionnaires and attachments into electronic form for storage and retrieval;
- the Defense Clearance and Investigations Index, which integrates the system's applications with the central index of all DoD personnel security investigations and clearances; and
- the Industrial Security System, which is a separate application that shares information in the corporate database.

The CCMS did not operate as intended. Instead of expediting the transmission of requests for investigations and reports to and from DSS field offices, system problems caused serious delays in information processing and resulted in a dramatic drop in the number of investigative cases opened and field investigations conducted.

Objectives

During our audit to determine the status of actions taken within the DoD relating to access reciprocity between special access programs, we identified problems with obtaining security clearances that affected individuals' access to special

access programs and all DoD operations. Our specific audit objective was to determine the effectiveness of the DSS process for tracking security clearance requests. We also reviewed the adequacy of the management control program as it applied to the specific audit objective. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program. See Appendix B for prior coverage related to the audit objectives.

Tracking Security Clearance Requests

The DSS lacked an effective means for tracking security clearance requests because existing systems and processes were inadequate for that purpose. As a result, DSS could not notify the requesting agencies of the status of its requests and the following situations existed.

- DSS could not identify, on a case-by-case basis, why 12,354 of 302,352 electronic requests received did not result in investigative cases. DSS stated possible reasons such as changes in type of investigation, duplicate submissions, conversions and reinstatements of prior clearances, and rejections.
- DSS could not specifically identify why 51,788 of 261,361 investigative cases were opened without electronic requests. DSS attributed these cases to changes in type of investigation, requests received in paper rather than electronically, and cases being reopened because of additional information requested by the adjudicative facility.
- Case analysts manually entering paper requests submitted into the Case Control Management System.
- Requesting agencies submitting duplicate requests that case analysts had to manually annotate as deleted.
- Because DSS did not actively acknowledge requests received, it appeared to requesting agencies that requests were lost.
- DSS estimated that its case analysts spent an excessive amount of their time researching the status of requests.

Clearance Requests Processing Time

DSS received security clearance requests in two forms: electronic and paper. Electronic personnel security questionnaires were automatically loaded into the CCMS. Case analysts manually entered personnel security questionnaires submitted on paper into the CCMS, which process bypasses the CCMS load gateway. A November 2, 1998, Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum directed all DoD organizations to use the electronic personnel security questionnaire by January 1, 1999, because it automatically edits and implements quality control and allows personnel security data to be transmitted electronically.

Once the security clearance request was loaded, a combination of computer and human tasks was used to review and identify investigative leads. When the request was properly validated, an investigative case was opened in the CCMS, required work was assigned to the field-operating locations, and a case was

opened in the Defense Clearance and Investigations Index. When the investigation was complete, the case was closed in CCMS and a Report for Adjudication was printed and sent to the appropriate facility for adjudication. During February 2000, a security clearance took an average of 109 days to be opened in CCMS.

Tracking Process

The DSS process for tracking security clearance requests was ineffective because there was not a one-to-one relationship between requests received and investigative cases opened. DSS did not open investigative cases for all requests received, nor did they receive electronic requests for every investigative case opened. DSS did not track the requests that did not open as investigative cases or the investigative cases that opened without electronic requests.

We calculated the monthly number of pending cases by using figures reported in the DSS monthly case reports between July and December 1999 (see Appendix C). During the 6 month period, 302,352 electronic requests were loaded and 261,261 cases were opened in the CCMS. We added the number of loaded requests to the prior month's number of pending cases and subtracted the number of closed cases to calculate the pending cases. We compared our calculated pending figures with the number of pending cases reported on the DSS monthly case reports. The calculated pending cases differed from the DSS reported pending cases. The differences between our calculated pending cases and the DSS reported pending cases showed that 12,354 cases disappeared from the DSS reports (see Table 1). DSS officials stated that these requests had not been opened as investigative cases. In addition, the differences showed 51,788 cases in which no requests were received for the pending investigation (see Table 2). DSS officials stated that these were investigative cases opened without electronic requests and therefore would not have a recorded load date.

Requests Not Opened as Investigative Cases. From July through December 1999, 12,354 of 302,352 electronic requests were not opened as investigative cases (see Table 1). DSS officials gave five possible reasons for not opening an electronic request as an investigative case, but they could not specify which reason for each of the 12,354.

- Case type changes – The type of investigation requested changed. For example, the requesting agency submitted a request for a Secret clearance, and then later submitted a second request for a Top Secret clearance for the same individual. One request never opened as an investigative case.
- Conversions – An individual left the Federal Government to work for a contractor. The contractor submitted a security clearance request. DSS determined that the Federal agency granted the individual a clearance and that the clearance was current within the past 2 years; therefore, DSS converted the clearance without opening a new investigation.

- Duplicates – The requesting agency submitted an identical request more than once.
- Reinstatements – An individual left one contractor and began working for another contractor. The new contractor submitted a security clearance request. DSS determined that the clearance was current within the past 2 years; therefore, it reinstated the clearance without opening a new investigation.
- Rejects – The requesting agency submitted an invalid or incomplete request. DSS returned the request for correction.

Table 1. Requests Not Opened As Investigative Cases

<u>Case Type</u>	<u>July</u>	<u>Aug.</u>	<u>Sept.</u>	<u>Oct.</u>	<u>Nov.</u>	<u>Dec.</u>	<u>Total</u>
Secret (new)						158	158
Secret PR ¹ (old)	77		248	136	56	4	521
Top Secret (new)		619	953	71	543	525	2,711
Top Secret PR ¹		148	639		508	537	1,832
Clearances	77	767	1,840	207	1,107	1,224	5,222
LAA ²			1				1
NACLC-T ³		2	8			41	51
OTHER	68	137	109	217	175	140	846
SAC ⁴	15	4			2	3	24
SII ⁵	2	27	87		4	7	127
Expanded NAC	75	162	148	244	184	260	1,073
Other investigations	160	332	353	461	365	451	2,122
AUTO-ENTNAC ⁶	1,211			25		66	1,302
ENTNAC ⁷				11	2,268	1,429	3,708
Total ENTNACs⁷	1,211			36	2,268	1,495	5,010
Total workload	1,448	1,099	2,193	704	3,740	3,170	12,354

¹Periodic Reinvestigation

²Limited Access Authorization

³National Agency Check with Local Agency Checks and Credit Check for Trustworthiness

⁴Spouse national Agency Check

⁵Special Investigative Inquiries

⁶Automated - Entrance National Agency Check

⁷Entrance National Agency Check

Investigative Cases Opened Without Electronic Requests. From July through December 1999, 51,788 of 261,361 investigative cases opened were opened without electronic requests (see Table 2). DSS officials provided three possible

reasons, but they could not specify which reason caused each of the 51,788 cases, although they estimated about 30,000 of the investigative cases resulted from paper requests.

- Case type change – The type of investigation requested changed. For example, the requesting agency submitted a request for a Secret clearance, then later submitted a request for a Top Secret clearance for the same individual.
- Paper requests – Security clearance requests received on paper were manually entered into the CCMS and missed the formal process of being loaded into the CCMS or counted as a loaded request.
- Reopened cases – An adjudication facility requested additional information to make an adjudicative decision. The case had already been closed in CCMS, so it had to be reopened to obtain the additional information.

Tracking Process. DSS should be able to track every security clearance request and to report the status of every request to the requesting agency. If DSS received 120 requests (100 electronic security clearance requests, 10 paper requests, and 10 requests to reopen cases) and opened 95 investigative cases, it should be able to report what happened to the remaining 25 requests; for example, 5 of the requests were conversions so DSS issued the converted clearance, 10 of the requests were duplicates so they were marked deleted, and 10 of the requests were rejected and returned to the requesting agencies.

DSS Unidentified Workload

DSS did not track all security clearance requests and did not notify requesting agencies of the status of their requests. The DSS workload and cost to perform investigations were affected by tasks not directly related to processing investigative cases. Case analysts were spending time manually entering paper requests into CCMS, requesting agencies were sending in duplicate requests, and the lack of active acknowledgement of request receipts created the appearance that requests were being lost. In addition, DSS estimated that its case analysts spent an excessive amount of their time researching the status of requests.

Manually Entering Paper Requests. Some requesting agencies did not have the capability to submit security clearance requests electronically; therefore, they submitted them on paper. Case analysts had to manually enter these paper requests into CCMS.

Duplicate Requests. Requesting agencies sent duplicate requests for clearances to DSS because they could not find an open case in the Defense Clearance and Investigations Index. DSS did not open a case in the Defense Clearance and Investigations Index until it was opened in CCMS, which in February 2000 was

taking an average of 109 days for security clearance requests. Case analysts had to manually review the requests to determine whether they were duplicates and then annotate the duplicate as deleted in CCMS.

Table 2. Investigative Cases Opened Without Electronic Requests

<u>Case Type</u>	<u>July</u>	<u>Aug.</u>	<u>Sept.</u>	<u>Oct.</u>	<u>Nov.</u>	<u>Dec.</u>	<u>Total</u>
Confidential	(51)	(9)	(31)	(538)	(6)	(132)	(767)
Confidential PR ¹	(21)	(7)	(39)	(26)	(20)	(18)	(131)
Secret (new)	(2,482)	(910)	(57)	(9,164)	(197)		(12,810)
Secret PR ¹ (new)	(1,160)	(344)	(981)	(966)	(590)	(514)	(4,555)
Secret PR ¹ (old)		(25)					(25)
Top Secret (new)	(1,318)						(1,318)
Top Secret PR ¹	(1,610)			(216)			(1,826)
Clearances	(6,642)	(1,295)	(1,108)	(10,910)	(813)	(664)	(21,432)
DCII-NAC ²	(1)		(1)	(3)	(3)		(8)
LAA ³		(1)		(1)			(2)
National Agency Check	(1,539)	(588)	(88)	(1,307)	(295)	(389)	(4,206)
NACLC-T ⁵	(10)			(71)	(78)		(159)
SAC ⁶			(8)	(17)			(25)
SII ⁷				(384)			(384)
Other investigations	(1,550)	(589)	(97)	(1,783)	(376)	(389)	(4,784)
AUTO-ENTNAC ⁸		(69)	(684)		(11)		(764)
ENTNAC ⁹	(760)	(7,661)	(16,387)				(24,808)
Total ENTNACs⁹	(760)	(7,730)	(17,071)		(11)		(25,572)
Total workload	(8,952)	(9,614)	(18,276)	(12,693)	(1,200)	(1,053)	(51,788)

¹Periodic Reinvestigation

²Defense Clearance and Investigations Index – National Agency Check

³Limited Access Authorization

⁵National Agency Check with Local Agency Checks and Credit Check for Trustworthiness

⁶Spouse national Agency Check

⁷Special Investigative Inquiries

⁸Automated - Entrance National Agency Check

⁹Entrance National Agency Check

Potential for Lost Requests. An increasing potential for losing requests existed because DSS did not have an effective tracking process. For example, in September 1999, DSS researched the status of 244 individuals for a Defense contractor and determined that there were no records for 52 of the individuals. DSS did not notify the Defense contractor that there were no records for the 52 individuals until our audit addressed the issue. In February 2000, DSS personnel stated that 49 of the 52 individuals had cases in process. DSS officials believed that the 49 individuals' requests had been received, but the investigative cases had not been opened in September 1999. DSS could not

determine what happened to the remaining three cases. DSS personnel have subsequently reviewed the status of cases that they had no record of and believe the electronic requests were not successfully transmitted to DSS. Therefore, they believe the cases were not lost, but never received.

DSS did not actively acknowledge receipt of electronic requests to the requesting agencies. However, DSS did not notify requesting agencies that unless the requesting agency could find the request on the DSS web site, then the request had not been successfully transmitted and received by DSS. Consequently, a requesting agency may have believed that its cases were being processed when in actuality DSS might never have received the request. In that situation, the requesting agency would be waiting indefinitely for a clearance that would never be granted because DSS had never received the request. Because DSS did not have an active acknowledgement of the request receipt, it appeared to requesting agencies that requests were being lost.

Researching Requests. DSS estimated that its case analysts were spending 30 to 40 percent of their time researching the status of requests for requesting agencies. In February 2000, DSS was taking an average of 109 days to open security clearance cases in CCMS and was not notifying the requesting agencies of their requests status, and the requesting agencies were calling and sending lists of individuals to DSS inquiring about their status.

DSS Workload. Changing the type of investigation, reopening cases, entering paper requests, deleting duplicate requests, reviewing and returning invalid and incomplete requests, and researching the status of requests required manual intervention by the case analysts, which affected the DSS workload. However, the work performed was not counted as part of the DSS workload, which was defined by cases processed and typically was reflected by the number of cases closed. Not including this work as part of the workload was a detriment to DSS when it needed to account for its resources and budget. The number of case analysts needed, based on the actual workload, was greater than reflected. If DSS tracked all security clearance requests, it would have a true picture of the overall workload and could more accurately support required resources and budget.

Extranet for Security Professionals

The Extranet for Security Professionals (ESP) program was conceived to provide a secure virtual community to aid in extra-organizational communication. A fundamental aim of the project was to create a collaborative environment for the national security community using Internet technologies without compromising security. The ESP concentrates on creating tools that allow users to populate the environment with information that they feel is important. The ESP was designed to provide core tools to support any community that has a need to collaborate across organizational or geographic boundaries that traditionally prevented, or made difficult, structured collaboration. Virtual Security Offices allow the organizations in the 13,000 cleared facilities a safe haven out of the public eye to create, manage, and share content with the rest of the national security community. The Virtual

Security Office allows each member organization to remotely manage its content by uploading and deleting files and managing access to its information, all using strong encryption.

Joint Security Commission II. The Report of the Joint Security Commission II, August 24, 1999, states:

Effective security that has reciprocity as a key component requires effective communications among those responsible for administering it. Such communications are important for activities ranging from policy coordination to rapid announcement of changes to day-to-day tasks such as clearance passing and access verification. The Extranet for Security Professionals (ESP), currently experimental, provides a vehicle for such communications. The experiment is proving successful. The ESP holds particular potential for resource savings through providing clearance and visit certification throughout Government and industry. Full development and continued operations and maintenance resourcing of the ESP, with attention to providing confidence in its future, should greatly expand its use and ensure the continued availability of what should prove to be an essential tool for more effective security.

Recommendation No. 19: The SPB [*Security Policy Board*] should continue to support the ESP, ensuring its continued development, funding, and eventual operational status.

Access to the ESP. All Defense and contractor security offices, which are the requesting agencies, have access to the ESP. The easiest and quickest way for requesting agencies to check the status of their requests is to check the status themselves. If cases in process at DSS were posted to the ESP, all requesting agencies could access the ESP and find the status of its requests. This would reduce the number of inquiries and duplicate requests from the requesting agencies.

Conclusion

Posting to the ESP. In February 2000, DSS was taking an average of 109 days to open security clearance cases. The requesting agencies were not receiving any notification that its requests were being processed until the cases were opened in CCMS and the Defense Clearance and Investigations Index. It would be beneficial to the requesting agencies to quickly know the status of their requests at the earliest time after they are loaded into CCMS. Posting the names and social security numbers of all cases in process on the ESP would allow requesting agencies to quickly check the status of their DSS requests. The ESP should contain the date a request was loaded into CCMS and the dates that a case was opened and closed. Posting this information on the ESP should dramatically reduce the amount of time that the case analysts are spending researching the status of requests and the number of duplicate requests that the requesting agencies are submitting, thereby allowing the case analysts' time to be spent in processing cases.

Tracking Requests. Tasks performed that do not directly relate to processing investigative cases, such as processing requests that are never opened and researching the status of requests, should be included in the workload. DSS would then have an accurate picture of its overall workload to support its required resources and budget. Tracking all security clearance requests would assist DSS in obtaining this objective.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Defense Security Service:

1. Track all security clearance requests from the time they are received until the investigative cases are opened. Security clearance requests that are not opened to investigative cases and those investigative cases that are opened without electronic requests should be included in the tracking process.

Defense Security Service Comments. The Director, DSS, concurred, stating that DSS needed an accurate picture of its overall workload. The Director appointed a working group to document the end-to-end process and account for all inputs from requests received through final disposition. The DSS database will be modified, but modification of the CCMS will take time and must be prioritized against other projected improvements.

Audit Response. Although the Director concurred, he did not provide estimated completion dates. Accordingly, we request that the Director, DSS, provide completion dates for its working group review and for the modifications to the CCMS in response to the final report.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director of Security, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred.

2. Post, weekly, the names and social security numbers of all cases in process on the Extranet for Security Professionals. The entry for each name should include, at a minimum, the date that the request was loaded into the Case Control Management System, the date that the investigative case was opened, and the date that the case was closed.

Defense Security Service Comments. The Director, DSS, concurred, stating that the dates an investigation is opened and closed are posted in the Defense Clearance and Investigations Index. In addition, DSS has established a site on its web site, which posts daily and maintains for 120 days an index of all electronic requests received. The requester must query the web site for acknowledgement of a successful receipt by DSS. Between the web site and the Defense Clearance and Investigations Index, authorized users can verify the status of the investigation. DSS will evaluate the possibility of adding the

investigation opening and closing dates and information on manually entered paper requests to the electronic request receipt web page. However, changes to the CCMS take time and must be prioritized with other improvements.

Audit Response. The Director's comments were generally responsive. DoD contractors, who are undergoing security clearance investigations, do not have access to the Defense Clearance and Investigations Index, but do have access to the web site. However, information on the status of cases or the manually entered paper requests was not posted to the web site. The DSS web site for electronic request receipts maintains requests for 120 days; however, in February 2000, the average days to close an investigation for a Secret or a Top Secret security clearance was from 211 to 306 days. Therefore, an inordinate amount of time would continue to be spent by DSS personnel investigating the status of requests. The Director's proposed actions are reasonable and we will follow up during our ongoing audit of the CCMS project.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Director of Security, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) partially concurred, stating that there should be a mechanism to monitor the status of requested investigations. However, funding for the Extranet for Security Professionals is problematic and the Joint Personnel Adjudication System, due to be implemented in the near future, will provide security managers with the capability to monitor investigations.

Audit Response. The comments of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) were generally responsive. As stated in the finding, the Report of the Joint Security Commission II, August 24, 1999, recommended that the Security Policy Board ensure funding of the Extranet for Security Professionals, which is operational and accessible by all security managers. The Joint Personnel Adjudication System's funding for FY 2000 was restored on March 31, 2000, by the Deputy Secretary of Defense; however, beta testing is scheduled August 2000 through December 2000 and full operational capability is not scheduled until FY 2002. Therefore, the Joint Personnel Adjudication System is not a readily available solution to eliminate the inordinate amount of time being expended by case analysts to determine the status of cases.

Appendix A. Audit Process

Scope

Work Performed. We evaluated the DSS process for tracking security clearance requests. We reviewed the number of cases loaded, opened, closed, and pending from October 1998 through December 1999. Because of a change in calculating pending cases, which was enacted in April but not implemented until July, we only reported from July 1999 through December 1999.

DoD-wide Corporate Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal, subordinate performance goals, and performance measures:

FY 2001 DoD Corporate Level Goal 2: Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineering the Department to achieve a 21st century infrastructure. **(00-DoD-2) Subordinate Performance Goal 2.1:** Recruit, retain, and develop personnel to maintain a highly skilled and motivated force capable of meeting tomorrow's challenges **(00-DoD-2.1) FY 2000 Performance Measure 2.1.1:** Enlisted Recruiting. **(00-DoD-2.1.1) Subordinate Performance Goal 2.3:** Streamline the DoD infrastructure by redesigning the Department's support structure and pursuing business practice reforms. **(00-DoD-2.3) FY 2000 Performance Measure 2.3.1:** Percentage of the DoD Budget Spent on Infrastructure. **(00-DoD-2.3.1)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Defense Weapon System Acquisition, the Information Management and Technology, and the Military Personnel Management high-risk areas.

Methodology

To determine how DSS tracks security clearance requests, we interviewed personnel to determine how they identify requests that never opened. We also compared the number of cases pending in CCMS for the period from July through December 1999 with auditor calculations for the same time period, based on the number of cases loaded and closed.

Use of Computer-Processed Data. We relied on computer-processed data contained in the CCMS without performing tests of system general and application controls to confirm the reliability of the data. We did not establish reliability of the data because there is no other centralized source of security clearance requests data. Also, because of the large number of cases, we believe

that any error rate would be insignificant to the finding. Therefore, not establishing the reliability of the database will not materially affect the results of our audit.

Audit Type, Dates, and Standards. We conducted this economy and efficiency audit from September 1999 through February 2000, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program

DoD Directive 5010.38, "Management Control Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We reviewed the adequacy of DSS management controls over the personnel security investigations program. We also reviewed the results of management's self-evaluation of those management controls.

Adequacy of Management Controls. We identified material management control weaknesses for DSS as defined by DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. DSS management controls were not adequate to ensure an effective process for tracking security clearance requests. A copy of the report will be provided to the senior official responsible for management controls in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Adequacy of Management's Self-Evaluation. DSS officials identified its personnel security investigation process as an uncorrected material weakness. However, they did not identify the material management control weakness identified by the audit because they did not evaluate that stage of the process.

Appendix B. Prior Coverage

During the last 6 years, the Inspector General, DoD, issued four reports, and the General Accounting Office, the Joint Security Commission II, the Commission on Protecting and Reducing Government Secrecy, and the Joint Security Commission issued one report each on security clearance background investigations.

General Accounting Office

United States General Accounting Office Report No. NSIAD-00-12 (OSD Case No. 1901), "DoD Personnel, Inadequate Personnel Security Investigations Pose National Security Risks," October 27, 1999.

Inspector General, DoD

Inspector General, DoD, Report No. D-2000-111, "Security Clearance Investigative Priorities," April 5, 2000.

Inspector General, DoD, Report No. D-2000-072, "Expediting Security Clearance Background Investigations for Three Special Access Programs" (U), January 31, 2000. (SECRET)

Inspector General, DoD, Report No. 98-067, "Access Reciprocity Between DoD Special Access Programs" (U), February 10, 1998. (CONFIDENTIAL)

Inspector General, DoD, Report No. 97-196, "Personnel Security in the Department of Defense," July 25, 1997.

Others

Joint Security Commission II, "Report of the Joint Security Commission II," August 24, 1999.

Commission on Protecting and Reducing Government Secrecy, Senate Document 105-2, "Report of the Commission on Protecting and Reducing Government Secrecy," March 3, 1997.

Joint Security Commission, "Redefining Security," February 28, 1994.

Appendix C. Auditor Calculations of Pending Cases

July Calculations

Case Type	June Pending	July Loaded	July Closed	Canceled		Calc ¹ Pending	July Pending	Calc ¹ - DSS Diff. ²
				Over 5 Days	Under 5 Days			
Confidential	1,408	337	91	4	-	1,650	1,701	(51)
Confidential PR ³	94	59	23	-	-	130	151	(21)
Secret (new)	36,233	8,599	2,841	96	3	41,892	44,374	(2,482)
Secret (old)	51	-	-	-	-	51	51	-
Secret PR ³ (new)	9,940	2,723	1,290	10	-	11,363	12,523	(1,160)
Secret PR ³ (old)	2,544	57	174	6	-	2,421	2,344	77
Top Secret (new)	34,281	5,681	1,786	229	5	37,942	39,260	(1,318)
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	24,593	4,049	1,430	69	6	27,137	28,747	(1,610)
Clearances	109,203	21,505	7,635	414	14	122,645	129,210	(6,565)
DCII-NAC ⁴	7	-	1	-	-	6	7	(1)
LAA ⁵	11	-	-	-	-	11	11	-
NAC ⁶	12,989	2,039	1,781	29	2	13,216	14,755	(1,539)
NACLC-T ⁷	56	42	12	1	-	85	95	(10)
OTHER	168	192	4	-	-	356	288	68
SAC ⁸	62	22	8	-	-	76	61	15
SII ⁹	1,263	317	41	12	-	1,527	1,525	2
XNAC ¹⁰	1,669	202	126	15	-	1,730	1,655	75
Other investigations	16,225	2,814	1,973	57	2	17,007	18,397	(1,390)
AUTO-ENTNAC ¹¹	19,401	19,532	13,536	6	-	25,391	24,180	1,211
ENAC ¹²	6,977	2,016	409	7	2	8,575	9,335	(760)
Total ENTNACs¹²	26,378	21,548	13,945	13	2	33,966	33,515	451
Total workload	151,806	45,867	23,553	484	18	173,618	181,122	(7,504)

Note. See the footnotes at the end of the appendix

August Calculations

Case Type	July Pending	August Loaded	August Closed	Canceled		Calc ¹ Pending	August Pending	Calc ¹ - DSS Diff. ²
				Over 5 Days	Under 5 Days			
Confidential	1,701	393	89	4	-	2,001	2,010	(9)
Confidential PR ³	151	66	21	2	-	194	201	(7)
Secret (new)	44,374	8,206	2,935	161	3	49,481	50,391	(910)
Secret (old)	51	-	-	-	-	51	51	-
Secret PR ³ (new)	12,523	3,476	1,724	21	1	14,253	14,597	(344)
Secret PR ³ (old)	2,344	57	147	1	-	2,253	2,278	(25)
Top Secret (new)	39,260	5,061	1,779	260	2	42,280	41,661	619
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	28,747	5,418	1,523	94	2	32,546	32,398	148
Clearances	129,210	22,677	8,218	543	8	143,118	143,646	(528)
DCII-NAC ⁴	7	-	-	1	-	6	6	-
LAA ⁵	11	5	-	-	-	16	17	(1)
NAC ⁶	14,755	2,186	1,027	31	2	15,881	16,469	(588)
NACLC-T ⁷	95	3	4	-	-	94	92	2
OTHER	288	123	4	1	-	406	269	137
SAC ⁸	61	12	3	1	-	69	65	4
SII ⁹	1,525	239	45	12	2	1,705	1,678	27
XNAC ¹⁰	1,655	171	103	10	-	1,713	1,551	162
Other investigations	18,397	2,739	1,186	56	4	19,890	20,147	(257)
AUTO-ENTNAC ¹¹	24,180	13,052	17,827	8	-	19,397	19,466	(69)
ENTNAC ¹²	9,335	2,179	108	12	2	11,392	19,053	(7,661)
Total ENTNACs¹²	33,515	15,231	17,935	20	2	30,789	38,519	(7,730)
Total workload	181,122	40,647	27,339	619	14	193,797	202,312	(8,515)

Note See the footnotes at the end of the appendix

September Calculations

Case Type	August Pending	Sept Loaded	Sept Closed	Canceled		Calc ¹ Pending	Sept Pending	Calc ¹ - DSS Diff. ²
				Over 5 Days	Under 5 Days			
Confidential	2,010	483	95	5	-	2,393	2,424	(31)
Confidential PR ³	201	60	11	-	-	250	289	(39)
Secret (new)	50,391	11,821	2,345	169	2	59,696	59,753	(57)
Secret (old)	51	-	-	-	-	51	51	-
Secret PR ³ (new)	14,597	5,709	1,357	11	-	18,938	19,919	(981)
Secret PR ³ (old)	2,278	-	81	9	1	2,187	1,939	248
Top Secret (new)	41,661	6,881	1,512	303	7	46,720	45,767	953
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	32,398	8,706	1,176	88	2	39,838	39,199	639
Clearances	143,646	33,660	6,577	585	12	170,132	169,400	732
DCII-NAC ⁴	6	-	1	-	-	5	6	(1)
LAA ⁵	17	1	-	-	-	18	17	1
NAC ⁶	16,469	3,789	1,533	45	8	18,672	18,760	(88)
NACLC-T ⁷	92	1	3	-	-	90	82	8
OTHER	269	230	4	-	1	494	385	109
SAC ⁸	65	7	7	-	-	65	73	(8)
SII ⁹	1,678	263	39	18	-	1,884	1,797	87
XNAC ¹⁰	1,551	347	132	23	-	1,743	1,595	148
Other investigations	20,147	4,638	1,719	86	9	22,971	22,715	256
AUTO-ENTNAC ¹¹	19,466	10,578	13,788	12	-	16,244	16,928	(684)
ENTNAC ¹²	19,053	9,914	141	105	20	28,701	45,088	(16,387)
Total ENTNACs¹²	38,519	20,492	13,929	117	20	44,945	62,016	(17,071)
Total workload	202,312	58,790	22,225	788	41	238,048	254,131	(16,083)

Note See the footnotes at the end of the appendix

October Calculations

<u>Case Type</u>	<u>Sept Pending</u>	<u>October Loaded</u>	<u>October Closed</u>	<u>Canceled</u>		<u>Calc¹ Pending</u>	<u>October Pending</u>	<u>Calc¹ - DSS Diff.²</u>
				<u>Over 5 Days</u>	<u>Under 5 Days</u>			
Confidential	2,424	502	207	9	-	2,710	3,248	(538)
Confidential PR ³	289	45	19	-	-	315	341	(26)
Secret (new)	59,753	11,897	4,360	336	11	66,943	76,107	(9,164)
Secret (old)	51	-	-	-	-	51	51	-
Secret PR ³ (new)	19,919	4,390	1,507	19	-	22,783	23,749	(966)
Secret PR ³ (old)	1,939	-	471	5	-	1,463	1,327	136
Top Secret (new)	45,767	5,221	2,758	371	7	47,852	47,781	71
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	39,199	5,193	1,965	156	7	42,264	42,480	(216)
Clearances	169,400	27,248	11,287	896	25	184,440	195,143	(10,703)
DCII-NAC ⁴	6	-	2	-	-	4	7	(3)
LAA ⁵	17	-	-	-	-	17	18	(1)
NAC ⁶	18,760	5,762	1,754	41	2	22,725	24,032	(1,307)
NACLC-T ⁷	82	-	9	-	-	73	144	(71)
OTHER	385	239	6	-	-	618	401	217
SAC ⁸	73	15	14	1	-	73	90	(17)
SII ⁹	1,797	245	70	40	1	1,931	2,315	(384)
XNAC ¹⁰	1,595	303	97	18	-	1,783	1,539	244
Other investigations	22,715	6,564	1,952	100	3	27,224	28,546	(1,322)
AUTO-ENTNAC ¹¹	16,928	9,253	9,734	8	-	16,439	16,414	25
ENTNAC ¹²	45,088	11,433	387	75	3	56,056	56,045	11
Total ENTNACs¹²	62,016	20,686	10,121	83	3	72,495	72,459	36
Total workload	254,131	54,498	23,360	1,079	31	284,159	296,148	(11,989)

Note. See the footnotes at the end of the appendix

November Calculations

Case Type	October Pending	Nov Loaded	Nov Closed	Canceled		Calc ¹ Pending	Nov Pending	Calc ¹ - DSS Diff. ²
				Over 5 Days	Under 5 Days			
Confidential	3,248	393	192	22	-	3,427	3,433	(6)
Confidential PR ³	341	21	34	1	-	327	347	(20)
Secret (new)	76,107	16,532	3,918	459	4	88,258	88,455	(197)
Secret (old)	51	-	1	-	-	50	50	-
Secret PR ³ (new)	23,749	4,577	1,922	32	-	26,372	26,962	(590)
Secret PR ³ (old)	1,327	-	122	6	-	1,199	1,143	56
Top Secret (new)	47,781	5,407	2,221	362	11	50,594	50,051	543
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	42,480	4,881	1,625	137	1	45,598	45,090	508
Clearances	195,143	31,811	10,035	1,019	16	215,884	215,590	294
DCII-NAC ⁴	7	-	1	-	2	4	7	(3)
LAA ⁵	18	-	-	-	-	18	18	-
NAC ⁶	24,032	5,729	1,401	79	-	28,281	28,576	(295)
NACLC-T ⁷	144	-	5	-	-	139	217	(78)
OTHER	401	220	2	2	-	617	442	175
SAC ⁸	90	24	9	1	-	104	102	2
SII ⁹	2,315	208	58	26	1	2,438	2,434	4
XNAC ¹⁰	1,539	412	58	14	-	1,879	1,695	184
Other investigations	28,546	6,593	1,534	122	3	33,480	33,491	(11)
AUTO-ENTNAC ¹¹	16,414	11,432	9,778	42	-	18,026	18,037	(11)
ENTNAC ¹²	56,045	6,334	447	194	3	61,735	59,467	2,268
Total ENTNACs¹²	72,459	17,766	10,225	236	3	79,761	77,504	2,257
Total workload	296,148	56,170	21,794	1,377	22	329,125	326,585	2,540

Note See the footnotes at the end of the appendix

December Calculations

Case Type	Nov	Dec	Dec	Canceled		Calc ¹	Dec	Calc ¹
	Pending	Loaded	Closed	Over 5 Days	Under 5 Days	Pending	Pending	- DSS Diff. ²
Confidential	3,433	407	116	6	-	3,718	3,850	(132)
Confidential PR ³	347	18	24	-	-	341	359	(18)
Secret (new)	88,455	14,919	2,720	232	6	100,416	100,258	158
Secret (old)	50	-	-	-	-	50	50	-
Secret PR ³ (new)	26,962	4,232	1,817	13	2	29,362	29,876	(514)
Secret PR ³ (old)	1,143	-	44	4	-	1,095	1,091	4
Top Secret (new)	50,051	4,279	989	158	3	53,180	52,655	525
Top Secret (old)	59	-	-	-	-	59	59	-
Top Secret PR ³	45,090	4,240	868	58	3	48,401	47,864	537
Clearances	215,590	28,095	6,578	471	14	236,622	236,062	560
DCII-NAC ⁴	7	-	-	-	-	7	7	-
LAA ⁵	18	-	-	-	-	18	18	-
NAC ⁶	28,576	3,556	758	24	1	31,349	31,738	(389)
NACLC-T ⁷	217	1	5	1	-	212	171	41
OTHER	442	235	7	1	-	669	529	140
SAC ⁸	102	14	6	-	-	110	107	3
SII ⁹	2,434	144	32	16	-	2,530	2,523	7
XNAC ¹⁰	1,695	411	40	10	-	2,056	1,796	260
Other investigations	33,491	4,361	848	52	1	36,951	36,889	62
AUTO-ENTNAC ¹¹	18,037	10,639	11,791	5	-	16,880	16,814	66
ENAC ¹²	59,467	3,285	405	119	-	62,228	60,799	1,429
Total ENTNACs¹²	77,504	13,924	12,196	124	-	79,108	77,613	1,495
Total workload	326,585	46,380	19,622	647	15	352,681	350,564	2,117

¹ Calculated

² Difference

³ Periodic Reinvestigation

⁴ Defense Clearance and Investigations Index – National Agency Check

⁵ Limited Access Authorization

⁶ National Agency Check

⁷ National Agency Check with Local Agency Checks and Credit Check for Trustworthiness

⁸ Spouse national Agency Check

⁹ Special Investigative Inquiries

¹⁰ Expanded National Agency Check

¹¹ Automated Entrance National Agency Check

¹² Entrance National Agency Check

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
 Director, Special Programs
 Director, Defense Logistics Studies Information Exchange
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
 Director, Security
Under Secretary of Defense (Comptroller)
 Deputy Chief Financial Officer
 Deputy Comptroller (Program/Budget)

Department of the Army

Chief, Army Technology Management Office
Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Director, Special Programs Division, Chief of Naval Operations
Auditor General, Department of the Navy
Superintendent, Naval Post Graduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Director, Security and Special Programs Oversight, Administrative Assistant to the
 Secretary of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Logistics Agency
Director, Defense Security Service
 Inspector General, Defense Security Service
 Internal Control Officer, Defense Security Service
Director, National Security Agency
 Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

Non-Defense Federal Organizations

Office of Management and Budget
General Accounting Office
National Security and International Affairs Division
Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Members

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International
Relations, Committee on Government Reform
House Permanent Select Committee on Intelligence

Defense Security Service Comments



DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651



May 8, 2000

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE
ASSISTANT INSPECTOR GENERAL FOR AUDITING,
OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

SUBJECT: Audit Report on Tracking Security Clearance Requests (Project No 9AD-0046 04)

Reference: DoDIG Memorandum , dated March 31, 2000, subject as above

We agree that the Defense Security Service is currently unable to account for each specific action on security clearance requests from the time they are received until they are completed. The DSS Case Control Management System (CCMS), as currently designed, does not retain all historical information pertaining to a case between EPSQ/manual receipt and DCII opening/closing. The system does not retain data on change in case category, e.g. when a Secret clearance is upgraded to a Top Secret clearance, rejections, duplicate submissions, conversions, and reinstatements of prior clearances. DSS can, however, account for every investigation by SSN from opening through closing and disposition to the appropriate adjudicative element. Recognizing the importance of accountability required to support resource requirements and the potential Fee for Service (FFS) environment, DSS is taking steps to identify and collect this information as part of the Case Control Management System. Pending modifications to our automated systems, our Operations Research Office will work with Center personnel to explore manual tracking between EPSQ receipt and DCII entry.

With respect to your statement that case analysts were spending 30 to 40 percent of their time researching the status of requests, we did not feel the percentage was that high but did recognize that this activity was diverting attention from direct production. Case analysts no longer accomplish this function.

The following comments concerning the recommendations are provided.

Recommendation 1-

We concur that DSS should have an accurate picture of its overall workload to support its required resources and budget. I have appointed a working group to document the "end-to-end" process and account for all inputs from investigative request received through final disposition. Our current database will be modified to retain all pertinent historical information (including dates/times for every occurrence - i.e. deletions, case type changes, cancellations, duplicates, conversions, reinstatements, etc.). This effort will take time and must be prioritized against other

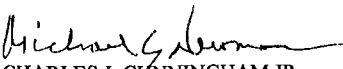
projected improvements to the Case Control Management System (CCMS) The DSS Operations Research Office will work with the Centers to capture this information

Recommendation 2 -

We concur that it would benefit the requesting agencies to receive acknowledgement of receipt of a request for an investigation To provide this information, DSS has established a site (<https://client.dss.mil>) on the DSS web site (www.dss.mil) which posts daily and maintains for 120 days, an index of all EPSQs received At this time, a requester must query the web site to receive an acknowledgement of a successful transmission We will look into the technical aspects of automating this process without requester action Information on the date an investigation is opened and closed is posted in the DCII and available to authorized users Between this web site and the DCII, security officers and authorized users can verify the status of investigations We will evaluate the possibility of adding the date the investigation was opened and the date that the investigation was closed to the EPSQ receipt web site, along with information on manual requests Actions that require changes to the CCMS will take time and must be prioritized with other improvements

DSS is well on its way to stabilizing its operations and will show a definite turn around in the third quarter of this fiscal year Our output has already increased dramatically As process and CCMS enhancements reduce our administrative processing time, there will be less need for the above information

If you have any questions, please contact Ms Janice Fielder, Acting Deputy Director for Standards and Quality, at 703-325-5277


for CHARLES J. CUNNINGHAM JR.
Director

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

MAY 10 2000



MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE,
OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

SUBJECT: Audit Report on Tracking Security Clearance Requests (Project No 9AD-0046 04)

This office has reviewed the draft report and offers the following comments:

1. **Recommendation 1: Track all security clearance requests from the time they are received until the investigative cases are opened. Security clearance requests that are not opened to investigative cases and those investigative cases that are opened without electronic requests should be included in the tracking records.**
 - Concur with the recommendation.
2. **Recommendation 2: Post, weekly, the names and social security numbers of all cases in process on the Extranet for Security Professionals. The entry for each name should include, at a minimum, the date that the request was loaded into the Case Control Management System, the date that the investigative case was opened, and the date that the case was closed.**
 - Partially concur with this recommendation. We agree that there should be a mechanism to monitor the status of requested investigations. However, the Extranet for Security Professionals (ESP) is not the appropriate one. The Department is due to implement the Joint Personnel Adjudication System (JPAS) in the near future. This will provide security managers (government and industry) the capability to monitor the status of requested investigations. Funding for the ESP continues to be problematic. As a discretionary program the DoD cannot rely on guaranteed continuation of ESP. Therefore, in our view, reliance on ESP as recommended is a quick fix without sustainability.

Richard F. Williams, CPP
Director of Security

cc:
DSS

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble

Mary L. Ugone

Robert K. West

Lois A. Therrien

Ellen P. Neff